PKI and DCE Within ASCI

Presented to DOE Security Research Workshop III

March 19, 1998

Frank Ploof

LLNL/AIS

A Comparison of DCE and PKI Technologies

C. Douglas Brown

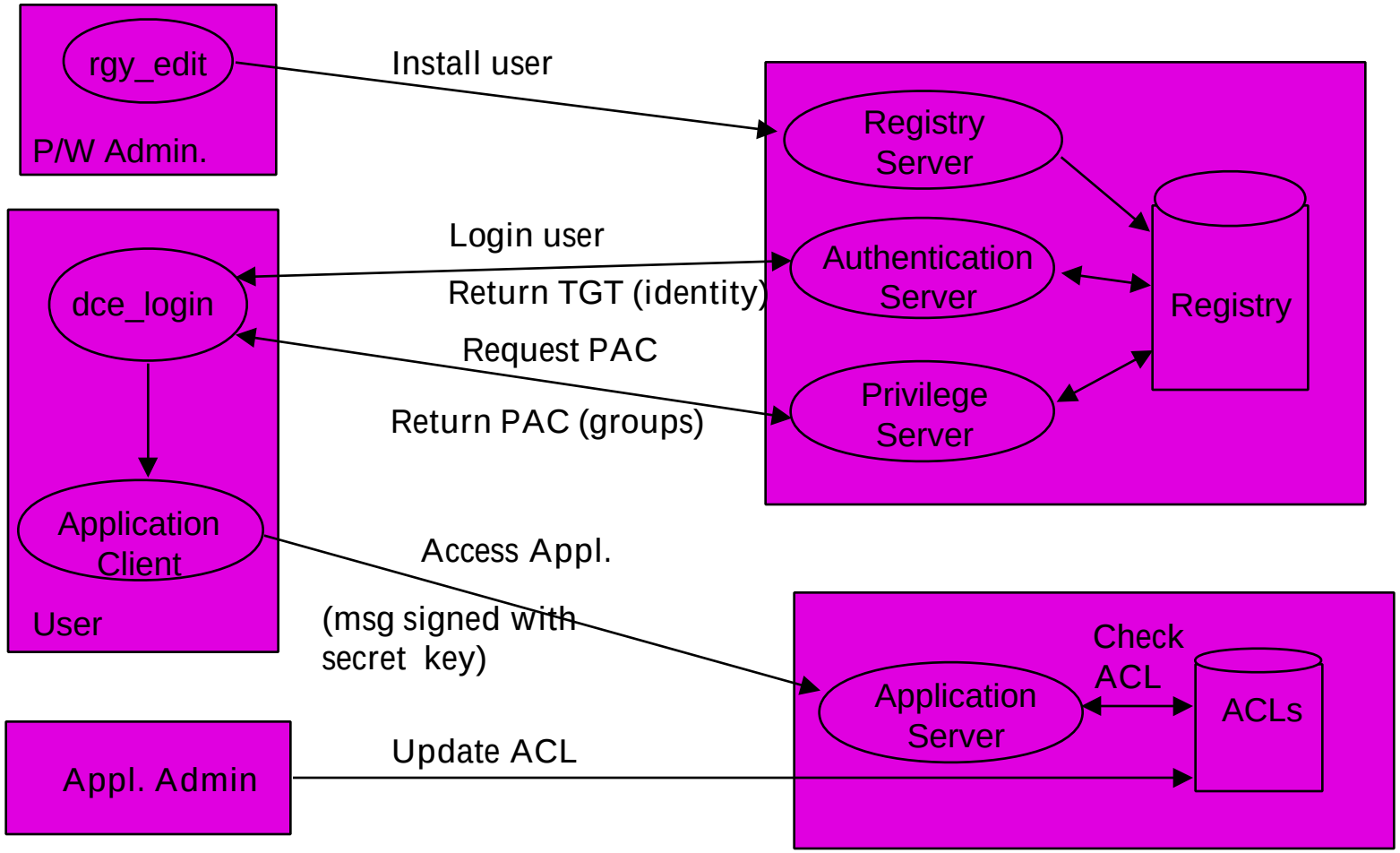
Sandia National Laboratories

for NWIG NTK Working Group Meeting

February 10-12, 1998

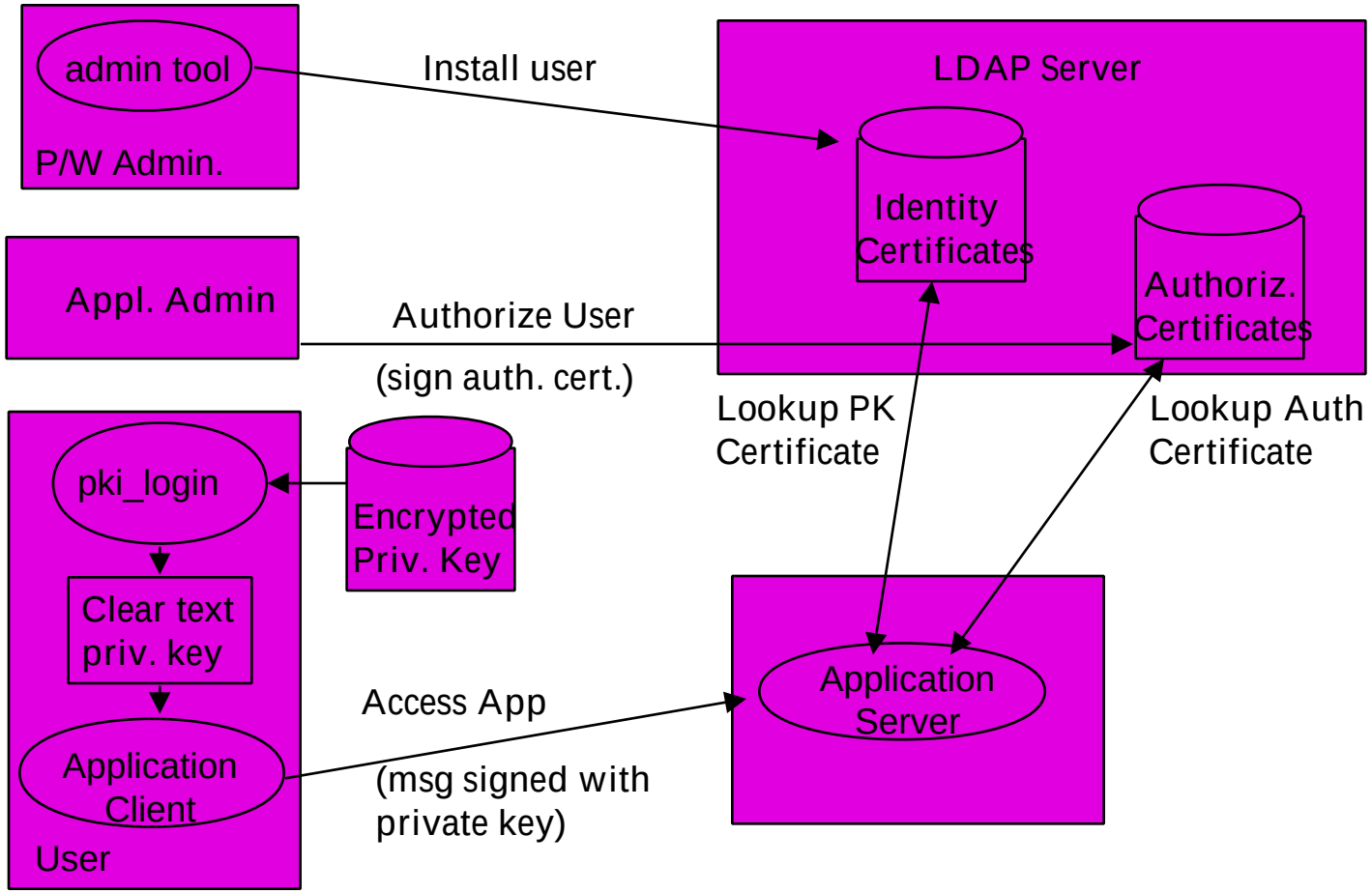
DCE Security Interactions

Sandia National Laboratories



PKI Security Interactions

Sandia National Laboratories



PKI Advantages

Sandia National Laboratories

- Decentralized key storage - no single repository of secret or private keys
- Supports NTK discretionary access control model
  - PK encrypted data not susceptible to unauthorized access by privileged administrators
  - In production today for Entrust encrypted e-mail
  - Might be possible using current technology for NTK protection of web objects (with Netscape plug-in for Entrust)

PKI Advantages (cont.)

Sandia National Laboratories

Computer Security Technology

- Smart-card compatibility
  - Many vendor supported systems available that secure the private key on smart card
  - Two factor authentication ("something you have + something you know")
  - Confiscation of hardware assures revokation of NTK access rights.
  - But – Smartcard hardware is evolving rapidly
  - PKCS11 helps, (not clear that PKCS11 spec is sufficient for plug-compatibility between different hardware choices.)

PKI Advantages (cont.)

- Non-repudiation Features
  - Authentication records or access records involving digitally signed forms can't be tampered with. You can take them to court.
  - Extremely strong non-repudiation when keys are isolated to PIN protected hardware tokens.
- But -- Most real world systems require at least a daily CRL lookup from a trusted central service.

PKI Advantages (cont.)

- The likely de-facto standard for HTTP authentication is PKI and SSL3 (TLS)
  - Basis for Netscape's single web sign-on strategy
  - Supported today using Netscape and Entrust
  - Currently the only choice other than Basic Authentication that will be supported by both Netscape and Microsoft web servers and browsers.
  - Will support "informed signing" of HTML form data submitted to a server.

PKI Advantages (cont.)

Sandia National Laboratories

Computer Security Technology

- Is the current standard for SSL server authentication and signed HTML executable content (Java, active X, javascript)
  - 22,000 Verisign SSL server certificates in existence
- Could support Bill Johnston's "Use-Condition" Security Architecture at LBL
  - Highly flexible authorization based on a mapping of attributes in PKI capability certificates to use-conditions imposed by resource owner
  - verifiably secure
  - In proof-of-concept stage today (see http://www-itq.lbl.gov/~johnston)

Footnote

PKI Disadvantages

Sandia National Laboratories

- No standard for PKI authorization
  - industry standards and DOE requirements still evolving
- Immature
  - few vendors
  - first products for authorization just now appearing
  - few examples of large-scale deployment
- Difficult and costly to deploy to desktops
- Cross-certification not yet blessed by SecureNet (for classified applications)

DCE Advantages

Sandia
National
Laboratories

- Based on standard code base available to OS vendors from a single source
- Based on mature authentication service (Kerberos)
- Designed for heterogeneous environments
  - works on UNIX, Windows 95, Windows NT, Mac
- Scalable and replicable security services
- Standard ACL mechanism for authorization

DCE Advantages (cont.)

Sandia National Laboratories

- Standard authorization mechanism
  - integrates with OS logon
  - familiar ACL paradigm (NTFS, DFS)
  - integrates with web object authorization systems
- Accreditation of DCE cross-cell authentication in process (nearing completion)

DCE Disadvantages

Sandia
National
Laboratories

- Not widely deployed
- No standard mechanism for Smartcards
- Lacks non-repudiation feature

PKI Authentication with DCE Credentials

Sandia National Laboratories

- Use PKI to get initial DCE credentials
- Existing vendor implementations
  - Gradient modified security service to trust certificates
  - Snareworks and IBM Global Sign-on store encrypted DCE keys in their security servers
- PKI support is priority for next version of DCE
  - will replace users secret keys with public/private key pairs for initial user authentication
- Integrates cleanly with existing DCE applications

Conclusions

Sandia National Laboratories

- DCE works now and provides convenient authorization mechanisms via ACLs and groups
- PKI is new, immature and developing rapidly
- PKI authentication with DCE offers some advantages in security and manageability
- Need to watch PKI technology, but it’s a bit early to jump into full-scale deployment

How Does DCE Authorization Work?

Sandia National Laboratories

- User logs in to DCE
  - user enters DCE password
  - obtains Kerberos ticket establishing his identity
  - obtains DCE Privilege Authorization Certificate (PAC) establishing group memberships
  - DCE credentials are encrypted via secret key unknown to the user but known to application server
- User accesses an object (e.g., DFS file)
  - presents DCE credentials (sent in RPC)
  - ACL manager checks user identity and groups against permissions in Access Control Lists

How Does PKI Authorization Work?

Sandia National Laboratories

- User logs in to application server
  - user enters password, unlocks private key
  - signs message (including timestamp and nonce) with private key and transmits to application server
  - may sent PK certificate along in login message
  - application server decrypts msg with user's public key

How Does PKI Authorization Work?

Sandia National Laboratories

- User accesses an object (e.g., web page)
  - application server looks up authorization certificate (signed by authorizing agent) via LDAP server
  - ACL manager checks user identity and groups against permissions in Access Control Lists